Christopher J. Schatz, OSB No. 915097
Assistant Federal Public Defender
101 SW Main Street, Suite 1700
Portland, OR 97204
Tel: (503) 326-2123
Fax: (503) 326-5524
Email: chris_schatz@fd.org

Ruben L. Iñiguez
Assistant Federal Public Defender
101 SW Main Street, Suite 1700
Portland, OR 97204
Tel: (503) 326-2123
Fax: (503) 326-5524
Email: ruben_iniguez@fd.org

Attorneys for Hock Chee Khoo

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA, **Plaintiff,** **vs.** **HOCK CHEE KHOO, et al.,** **Defendants.**	**CR 09-321-KI** **SUPPLEMENTAL DECLARATION OF COMPUTER FORENSICS EXPERT MICHAEL A. BEAN IN SUPPORT OF MOTION TO EXCLUDE IMAGES OF THE WU LAPTOP HARD-DRIVE.**

I, Michael Bean, declare:

1. I am an expert in computer forensics, and I have been recognized as such. I have testified as a computer forensics expert in both federal and state court.

2. I hereby refer to, and by such reference incorporate herein, all averments and statements set forth in my declaration [Docket No. 36] heretofore filed in the instant matter on May 28, 2010.

3. On November 10, 2010, I was advised by Federal Pubic Defender Computer Data Specialist Maija Wells that the Khoo defense team had learned that files named "Hoffman 200601.PST" and "Hoffman2005.PST"(or possibly "Hoffman200502.PST") which contained email, had been present on the Wu Laptop hard drive at the time Wu entered the United States on October 17, 2006.[1] More specifically, I was advised that these files had been created for the specific purpose of storing email messages exchanged between Wu and Lawrence "Drew" Hoffman during 2005 (Hoffman-2005.PST or Hoffman200502.PST) and the first six months of 2006 (Hoffman 200601.PST).

4. Based on this information, I conducted further analysis of the Forensic Tool Kit (FTK) EnCase image of the Wu Laptop hard drive made by the FBI searching for all three .pst files described in paragraph (3) above. The files on the hard drive go back in date to November of 1995. User based content started appearing in 2005. There are numerous files with created or written dates during the 2005 and 2006 time period.[2] There is no indication of any systematic attempt on the part of Wu, as the user of the Laptop, to delete Files created during 2005 or 2006; although, several of the 2005 files are marked "old."

[1] In computing, the .pst file extension refers to an open proprietary file format that is used to store copies of messages, calendar events, and other items within Microsoft software such as Microsoft Outlook.

[2] When data is entered into the computer to create a file, the electronic data constituting the file is date stamped with a file-creation date. Every time the file is opened and new data is entered, modifying the file, a file-written date is generated.

5. In the course of the review described in (4) above, I did make a very unusual discovery. The FTK EnCase image of the Wu Laptop hard drive contains only one file that is recorded as deleted and able to be recovered. This file is named "Ntuser.tmp" and it has a last accessed date of October 21, 2006 (China time), approximately 15 days after the image was purported to have been created by the FBI. This is also inconsistent with the date that the Acronis Backup copy of the Wu hard drive was made, which was October 18, 2006 (China time). This is unusual and surprising in that, during the course of normal computing, files (such as, for example, temporary files) are routinely and automatically deleted without user activity. Consequently, as an experienced forensic computer examiner I expect to find deleted files that are recoverable from unallocated space on the hard drive. The absence of deleted files detectable by forensic software as being recoverable leads me to believe with reasonable forensic certainty that, before the FBI imaged the hard drive, the Wu Laptop hard drive had been altered.

6. As a result of the unusual and surprising discovery described in (5) above, I conducted an analysis of the unallocated space of the FTK EnCase image of the Wu hard drive made which is where deleted file content resides.[3] The unallocated space contained what appeared to be deleted data in some areas but it also contained large blocks of blank or empty space which is consistent with specific targeted wiping or intentional defragmentation of the hard drive. Defragmentation of a hard drive can easily be accomplished using a utility named "Defrag" which is supplied with the Windows operating system. The file used to execute the "defrag" operation is named "Defrag.exe" and this

[3] Unallocated space refers to that portion of a hard drive disk sector that is not fully used by current allocated file data and which, consequently, may contain data from a previously deleted file that was not overwritten in its entirety by current file data.

file is located in the "Windows\System32" directory present in the image made by the FBI of the Wu Laptop hard drive.

7. Defragmentation of a hard drive is commonly used to optimize the speed of the operating system. It also increases the speed in which the computer is able to render requested data for view by the user of the computer. It is also used to remove fragmented content of deleted files. The "Defrag" operation removes the Master File Table (MFT) records of deleted files that are no longer recognized as occupying the reported storage locations on the drive. It also shifts active file content of active non-deleted files from their current fragmented locations to contiguous locations that are recognized as available for new content storage after the removal of the invalid MFT records.

8. Analysis of the dates and times associated with the file named "defrag.exe" located in the FTK EnCase image of the Wu hard drive revealed a last accessed date of October 18, 2006, at 11:44 a.m. (China Time) indicating that the defragmentation process was initiated on this date and at this time. This date and time is later than the installation of the Acronis backup software (October 18, 2006, at 2:14 a.m. China time) installed by Mark Hansen while the computer was in the possession of Mark Hansen. The installation of the Acronis software by Hansen in itself is an action that would have overwritten deleted content in the unallocated space.

9. Notwithstanding the discovery described in (5) above, I was able to recover over 17,000 items that had been deleted. This was accomplished by locating deleted MFT records in the unallocated space and then resolving the storage locations where the actual data was located which are stored in the recovered MFT records.

10. One of the folders recovered is named "Outlook." This folder contains a deleted file named "Hoffman 200601". Since the file has been deleted and the content of the unallocated space

has been shifted around during the defrag process, the file reports as corrupt when it is exported from the image and an attempt to open it using Outlook is made.[4] I was not able to locate the file named "Hoffman2005.PST". However, in my view it is reasonable to conclude that, given the discovery of the "Hoffman 200601.PST" file shell confirming the information received by the Khoo defense team, a similar file named "Hoffman2005.PST" or "Hoffman200502.PST" did exist on the laptop. Unfortunately, this file was subsequently deleted and then completely overwritten either during the defragmentation process or during the installation of the Acronis software by Hansen.

11. In a further attempt to recover the files named "Hoffman 200601.PST", "Hoffman2005.PST", and/or "Hoffman200502.PST", I conducted an analysis of the Acronis backup copy of the hard drive that was created by Mark Hansen. Inspection of the unallocated space contained in the Acronis Backup copy revealed no content at all. Since the unallocated content of the Wu Laptop hard drive was not captured or properly preserved in the Acronis backup copy or the FTK EnCase image, I have not been able to recover or detect the listed files.[5]

12. Given the state of the FTK EnCase Wu Laptop and Acronis backup copy images as containing manipulated and spoliated data, and/or data introduced into the Wu Laptop hard drive following its seizure by Hoffman on October 17, 2006, in my professional opinion as a forensic computer examiner, neither the FTK EnCase Wu Laptop hard drive image nor the Acronis backup copy image can be viewed as trustworthy repositories of data.

[4] Outlook is the native program used to open this type of file.

[5] There are 285 individual files that are reported as deleted/recoverable in the Acronis backup copy. However, these files are not present in the FTK EnCase image of the Wu hard drive created by the FBI.

I declare under perjury under the laws of the United States of America that the foregoing statements are true and correct to the best of my knowledge and belief, and that this Declaration was executed on November 12, 2010, in Portland, Oregon.

Michael Bean